REMARKS

I. Status Summary

Claims 1-134 are pending in the present application. Claims 1-29, 34-36, 41-43, 45-71, 76-78, 83-85, 87-92, 97, 98, 103, 104, 106-110, 116-118, 124-126, and 128-134 have been canceled. Claims 30, 37, 44, 72, 79, 86, 93, 99, 105, 111, 119, and 127 have been amended. New claims 135-150 have been added. Therefore, upon entry of this Amendment, claims 30-33, 37-40, 44, 72-75, 79-82, 86, 93-96, 99-102, 105, 111-115, 119-123, 127, and 135-150 will be pending. No new matter has been introduced by the present amendment. Reconsideration of the application as amended and based on the remarks set forth hereinbelow is respectfully requested.

Claims 32, 39, 74, 81, 96, 114, and 122 have each been amended to remove one of the occurrences of the phrase "simple mail transfer protocol".

II. Information Disclosure Statement

The Examiner states that the Information Disclosure Statement filed August 12, 2004 fails to comply with 37 C.F.R. § 1.98(a)(3) because it does not include a concise explanation of the relevance of each patent listed that is not in the English language. Copies of the English abstracts of the patents are enclosed herewith. The abstracts provide explanation of the relevance of each patent.

III. Specification

The disclosure stands objected to because of informalities. In particular, the Examiner states that the section heading "Description" should be removed from page 1. As set forth above, the specification has been amended to replace the heading "Description" at page 1, line 2, with the heading "Title". Applicants respectfully submit that the new heading is proper.

Further, the Examiner states that application serial numbers should be included with the named applications in the "Related Applications" section. As set forth above,

the specification has been amended to add application serial numbers to the named applications.

IV. Claim Rejections Under 35 U.S.C. § 102

Claims 1, 2, 5-12, 15-21, 24-31, 34-38, 41-45, 48-50, 65, 66, and 69-71 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,161,185 to Guthrie et al. (hereinafter, "Guthrie"). Further, claims 51-64 and 93-134 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,405,318 to Rowland (hereinafter, "Rowland"). Claims 72-92 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0135612 to Royer et al. (hereinafter, "Royer"). These rejections are respectfully traversed.

IV.A. Rejections Based Upon Guthrie

Claims 1, 2, 5-12, 15-21, 24-29, 34-36, 41-43, 45, 48-50, 65, 66, and 69-71 have been canceled. Accordingly, it is respectfully submitted that the rejection of claims 1, 2, 5-12, 15-21, 24-29, 34-36, 41-43, 45, 48-50, 65, 66, and 69-71 under 35 U.S.C. § 102(b) should be withdrawn.

Guthrie is directed to electronic access systems in computers. In particular, Guthrie discloses a client **102** and a server **104** exchanging messages and other data via a network **100**. (See column 4, lines 65 and 66, and Figures 1a and 1b, of Guthrie). Server **104** provides client **102** with messages indicating whether authentication requests succeed or fail. (See column 7, lines 35-45, of Guthrie). If the number of authorization failures is too high, the user may be locked out. (See column 8, lines 10-17, of Guthrie). Guthrie also discloses that server **104** may record audit information for each log-on attempt. An IP address contained in a message may provide an audit trail for authorization attempts. (See column 1, lines 46-65, of Guthrie).

Claim 30 recites a method for monitoring user login activity for a server application. Claim 30 has been amended to recite capturing communication data communicated in a network connecting a server application and a client. For example, Figure 1A shows a security system **102** operable to capture packets transmitted

- 32 -

between server **S** and clients **C1-C3** on communication network **CN**. Further, claim 30 recites monitoring user login failures between the server application and the client during a predetermined time and based on the captured communication data. Claim 30 also recites detecting whether the number of user login failures exceeds a predetermined number. Applicants respectfully submit that <u>Guthrie</u> fails to disclose each and every feature recited by claim 30.

As stated above, <u>Guthrie</u> discloses locking out a user if the number of authorization failures is too high. (See column 8, lines 10-17, of <u>Guthrie</u>). <u>Guthrie</u> also discloses that server **104** may record audit information for each log-on attempt. An IP address contained in a message may provide an audit trail for authorization attempts. (See column 1, lines 46-65, of <u>Guthrie</u>). However, <u>Guthrie</u> fails to disclose capturing communication data communicated in a network connecting a server application and a client, and monitoring user login failures based on the captured communication data, as recited by claim 30. Rather, <u>Guthrie</u> discloses maintaining the log-on attempt audit information at server **104** and analyzing the log-attempt data at server **104**. There is no disclosure of capturing the data in a network connecting the server application and client and analyzing the captured data. The claimed subject matter provides the advantage of passive capturing of communication data. Accordingly, applicants respectfully submit that the rejection of claim 30 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claim 31 depends upon claim 30. Therefore, claim 31 includes the features recited by claim 30. Accordingly, for the same reasons set forth above for claim 30, applicants respectfully submit that the rejection of claim 31 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claim 37 has been amended similar to claim 30. In particular, claim 37 recites a network interface operable to capture communication data communicated in a network connecting a server application and a client. Further, claim 37 recites a detector operable to monitor user login failures between the server application and the client during a predetermined time and based on the captured communicated data, and operable to detect when the number of user login failures exceeds a

predetermined number. As set forth above with respect to claim 30, <u>Guthrie</u> fails to disclose these features. In particular, <u>Guthrie</u> fails to disclose capturing the data in a network connecting the server application and client and analyzing the captured data. For these reasons, applicants respectfully submit that <u>Guthrie</u> fails to disclose each and every feature recited by claim 37. Accordingly, applicants respectfully submit that the rejection of claim 37 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 38 depends upon claim 37. Therefore, claim 38 includes the features recited by claim 37. Accordingly, for the same reasons set forth above for claim 37, applicants respectfully submit that the rejection of claim 38 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claim 44 has been amended similar to claim 30. In particular, claim 44 recites capturing communication data communicated in a network connecting a server application and a client. Further, claim 44 recites monitoring user login failures between the server application and the client during a predetermined time and based on the captured communication data. Claim 44 also recites detecting when the number of user login failures exceeds a predetermined number. As set forth above with respect to claim 30, <u>Guthrie</u> fails to disclose these features. In particular, <u>Guthrie</u> fails to disclose capturing the data in a network connecting the server application and client and analyzing the captured data. For these reasons, applicants respectfully submit that <u>Guthrie</u> fails to disclose each and every feature recited by claim 44. Accordingly, applicants respectfully submit that the rejection of claim 44 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

IV.B. Rejections Based upon Rowland

Claims 51-64, 97, 98, 103, 104, 106-110, 116-118, 124-126, and 128-134 have been canceled. Accordingly, it is respectfully submitted that the rejection of claims 51-64, 97, 98, 103, 104, 106-110, 116-118, 124-126, and 128-134 under 35 U.S.C. § 102(b) should be withdrawn.

Rowland is directed to an intrusion detection system and method that monitors a computer system for activity indicative of attempted or actual access by unauthorized persons or computers. Referring to Figure 1 of Rowland, an intrusion detection system **1** includes a log audit function **2**, a login anomaly detection function **3**, a logout anomaly detection **7**, a session monitor function **4**, and a port scan detector function **5** interfacing with a local controller function **6**. (See column 3, lines 32-37, of Rowland). Login anomaly detection function **3** monitors system login activity and when anomalous behavior is detected, notifies controller **6** and sends information about the activity to controller **6** for further processing. (See column 3, lines 48-51, of Rowland). Rowland also discloses checking a user login to determine if there are multiple concurrent logins for the same user. A multiple concurrent login means that a user is logged into the system more than once from one or more different hosts concurrently. (See column 5, lines 10-20, of Rowland).

Claim 93 recites a method for monitoring simultaneous logins for a server application. Claim 93 has been amended to recite capturing communication data communicated in a network connecting a server application and at least one client. Further, claim 93 has been amended to recite that the captured communication data is associated with first and second user login sessions for first and second users, respectively, of the server application. Claim 93 has also been amended to recite monitoring the captured communication data associated with the first and second user login sessions. Further, claim 93 recites determining whether the second user login session occurs during the first user login session when the user of the first and second login session are identical. Applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 93.

Rowland fails to disclose capturing communication data communicated in a network connecting a server application and at least one client where the captured communication data is associated with first and second user login session for first and second users, as recited by claim 93. Rather, Rowland discloses that the system onto which user's login maintains a record of login / logout activity and that this activity is monitored. There is no disclosure of capturing communication data from a network for

use in monitoring login sessions, as recited by claim 93. The claimed subject matter provides the advantage of passive capturing of communication data. Accordingly, for this reason, it is respectfully submitted that the rejection of claim 93 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 94-96 depend upon claim 93. Therefore, claims 94-96 include the features recited by claim 93. Accordingly, for the same reasons set forth above for claim 93, applicants respectfully submit that the rejection of claims 94-96 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 99 has been amended similar to claim 93. In particular, claim 99 has been amended to recite a network interface operable to capture communication data communicated in a network connecting a server application and at least one client. Further, claim 99 has been amended to recite that the captured communication data is associated with first and second user login sessions for the first and second users, respectively, of the server application. Claim 99 has also been amended to recite a detector operable to monitor the captured communication data associated with the first and second user login sessions, and operable to determine whether the second user login session occurs during the first user login session when the user of the first and second login session are identical. As set forth above with respect to claim 93, Rowland fails to disclose these features. In particular, Rowland fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 99. For these reasons, applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 99. Accordingly, applicants respectfully submit that the rejection of claim 99 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 100-102 depend upon claim 99. Therefore, claims 100-102 include the features recited by claim 99. Accordingly, for the same reasons set forth above for claim 99, applicants respectfully submit that the rejection of claims 100-102 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 105 has been amended similar to claim 93. In particular, claim 105 has been amended to recite capturing communication data communicated in a network

connecting a server application and at least one client. Claim 105 has also been amended to recite that the captured communication data is associated with first and second user login sessions for first and second users, respectively, of the server application. Further, claim 105 has been amended to recite monitoring the captured communication data associated with the first and second user login sessions. Claim 105 also recites determining whether the second user login session occurs during the first user login session when the user of the first and second login session are identical. As set forth above with respect to claim 93, Rowland fails to disclose these features. In particular, Rowland fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 105. For these reasons, applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 105. Accordingly, applicants respectfully submit that the rejection of claim 105 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claim 111 recites a method of monitoring logins for a server application. Further, claim 111 recites designating a first login time for a client as a disallowed login time. Claim 111 has been amended to recite determining a second login time for the client in communication data with a server application based on communication data captured from a network connecting the server application and the client. Further, claim 111 recites determining whether the second login time matches the first login time. Claim 111 also recites indicating that the client in data communication with the server application is logging in at a disallowed login time if the first and second login times match. Applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 111.

Rowland fails to disclose capturing communication data communicated from a network connecting a server application and a client, as recited by claim 111. Rather, Rowland discloses that the system onto which user's login maintains a record of login / logout activity and that this activity is monitored. Further, there is no disclosure of determining a second login time for the client in communication data with a server application based on communication data captured from a network connecting the server application and the client, as recited by claim 111. The claimed subject matter

provides the advantage of passive capturing of communication data. Accordingly, for this reason, it is respectfully submitted that the rejection of claim 111 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 112-115 depend upon claim 111. Therefore, claims 112-115 include the features recited by claim 111. Accordingly, for the same reasons set forth above for claim 111, applicants respectfully submit that the rejection of claims 112-115 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 119 has been amended similar to claim 111. In particular, claim 119 has been amended to recite a network interface operable to monitor and capture communication data communicated between a server application and a client. Further, claim 119 has been amended to recite a detector operable to designate a first login time for a client as a disallowed login time, operable to determine a second login time for the client in communication data with a server application based on the communication data captured from the network, operable to determine whether the second login time matches the first login time, and operable to indicating that the client in data communication with the server application is logging in at a disallowed login time, if the first and second login times match. As set forth above with respect to claim 111, Rowland fails to disclose these features. In particular, Rowland fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 119. For these reasons, applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 119. Accordingly, applicants respectfully submit that the rejection of claim 119 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 120-123 depend upon claim 119. Therefore, claims 120-123 include the features recited by claim 119. Accordingly, for the same reasons set forth above for claim 119, applicants respectfully submit that the rejection of claims 120-123 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 127 has been amended similar to claim 111. In particular, claim 127 recites designating a first login time for a client as a disallowed login time. Claim 127 has been amended to recite determining a second login time for the client in data

communication with a server application based on communication data captured from a network connecting the server application and the client. Further, claim 127 recites determining whether the second login time matches the first login time. Claim 127 recites indicating that the client in data communication with the server application is logging in at a disallowed login time if the first and second login times match. As set forth above with respect to claim 111, Rowland fails to disclose these features. In particular, Rowland fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 127. The claimed subject matter provides the advantage of passive capturing of communication data. For these reasons, applicants respectfully submit that Rowland fails to disclose each and every feature recited by claim 127. Accordingly, applicants respectfully submit that the rejection of claim 127 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

IV.C. Rejections Based Upon Royer

Claims 76-78, 83-85, and 87-92 have been canceled. Accordingly, it is respectfully submitted that the rejection of claims 76-78, 83-85, and 87-92 under 35 U.S.C. § 102(b) should be withdrawn.

Claim 72 recites a method for monitoring user logoff activity for a server application. Claim 72 has been amended to recite capturing communication data of a login session communicated in a network connecting a server application and a client. For example, Figure 1A shows a security system **102** operable to capture packets transmitted between server **S** and clients **C1-C3** on communication network **CN**. Further, claim 72 has been amended to recite monitoring user logoff between the server application and the client based on the captured communication data. Claim 72 has also been amended to recite monitoring automatic session expiration between the server application and the client based on the captured communication data. Further, claim 72 recites determining whether the client completes logoff before the session automatically expires. Applicants respectfully submit that Royer fails to disclose each and every feature recited by claim 72.

Royer discloses a system including concurrently operating applications **200** and **230**, a web browser **235**, and manager **250** using a system interoperability protocol. (See paragraph 0028 and Figure 2, of Royer). The applications may exchange and store information relating to logon and logoff of a web page managed by the system applications. (See paragraphs 0029 and 0030, of Royer). However, Royer fails to disclose capturing communication data of a login session communicated in a network connecting a server application and a client. There is no disclosure in Royer of capturing communication data from a network. The claimed subject matter provides the advantage of passive capturing of communication data. Further, there is no disclosure of monitoring user logoff and automatic session expiration between a server application and a client based on the captured communication data, as recited by claim 72. Accordingly, applicants respectfully submit that the rejection of claim 72 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 73-75 depend upon claim 72. Therefore, claims 73-75 include the features recited by claim 72. Accordingly, for the same reasons set forth above for claim 72, applicants respectfully submit that the rejection of claims 73-75 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 79 has been amended similar to claim 72. In particular, claim 79 has been amended to recite a network interface operable to capture communication data of a login session communicated in a network connecting a server application and a client. Further, claim 79 has been amended to recite a detector operable to monitor user logoff between the server application and the client based on the captured communication data, operable to monitor automatic session expiration between the server application and the client based on the captured communication data, and operable to determine whether the client completes logoff before the session automatically expires. As set forth above with respect to claim 72, Royer fails to disclose these features. In particular, Royer fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 79. For these reasons, applicants respectfully submit that Royer fails to disclose each and every feature

recited by claim 79. Accordingly, applicants respectfully submit that the rejection of claim 79 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

Claims 80-82 depend upon claim 79. Therefore, claims 80-82 include the features recited by claim 79. Accordingly, for the same reasons set forth above for claim 79, applicants respectfully submit that the rejection of claims 80-82 under 35 U.S.C. § 102(b) should be withdrawn and the claims allowed.

Claim 86 has been amended similar to claim 72. In particular, claim 86 recites capturing communication data of a login session communicated in a network connecting a server application and a client. Claim 86 has been amended to recite monitoring user logoff between the server application and the client based on the captured communication data. Further, claim 86 recites monitoring automatic session expiration between the server application and the client based on the captured communication data. Claim 86 recites determining whether the client completes logoff before the session automatically expires. As set forth above with respect to claim 72, Royer fails to disclose these features. In particular, Royer fails to disclose capturing communication data from a network for use in monitoring, as recited by claim 86. For these reasons, applicants respectfully submit that Royer fails to disclose each and every feature recited by claim 86. Accordingly, applicants respectfully submit that the rejection of claim 86 under 35 U.S.C. § 102(b) should be withdrawn and the claim allowed.

V. Claim Rejections Under 35 U.S.C. § 103

Claims 3, 4, 13, 14, 22, 23, 32, 33, 39, 40, 46, 47, 67, and 68 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Guthrie in view of U.S. Patent Application Publication No. 2002/0184217 to Bisbee et al (hereinafter, "Bisbee"). These rejections are respectfully traversed.

Claims 32 and 33 depend upon claim 30. Therefore, claims 32 and 33 include the features recited by claim 30. As set forth above, Guthrie fails to disclose each and every feature recited by claim 30. In particular, Guthrie fails to disclose capturing the

data in a network connecting the server application and client and analyzing the captured data, as recited by claim 30. Guthrie also fails to suggest this feature.

Bisbee fails to overcome the significant shortcomings of Guthrie. As set forth above, Bisbee discloses that logon component **234** is operable to generate a password for the user and securely stores the password. (See paragraph 0041, of Bisbee). Further, logon component **234** manages the logon process for a user. There is no disclosure or suggestion in Bisbee of capturing the data in a network connecting the server application and client and analyzing the captured data, as recited by claim 30.

For these reasons, applicants respectfully submit that Guthrie and Bisbee, either alone or in combination, fail to disclose or suggest each and every feature recited by claim 30. Accordingly, because claims 32 and 33 depend upon claim 30, it is respectfully submitted that the rejection of claims 32 and 33 under 35 U.S.C. § 103(a) should be withdrawn and the claims allowed.

Claims 39 and 40 depend upon claim 37. As set forth above, claim 37 has been amended similar to claim 30. Accordingly, for the reasons provided for claim 30, applicants respectfully submit that the rejection of claims 39 and 40 under 35 U.S.C. § 103(a) should be withdrawn and the claims allowed.

VI. Double Patenting

Claims 1-7, 11-17, and 20-26 stand objected to under 37 C.F.R. § 1.75 as being a substantial duplicate of claims 30-50. Claims 1-7, 11-17, and 20-26 have been canceled. Accordingly, the objection to claims 1-7, 11-17, and 20-26 should be withdrawn.

Claims 44-50 stand objected to under 37 C.F.R. § 1.75 as being a substantial duplicate of claims 65-71. Claims 65-71 have been canceled. Accordingly, the objection to claims 44-50 should be withdrawn.

VII. New Claims

New claims 135-150 have been added and depend upon one of claims 30, 37, 72, 79, 93, 99, 111, and 119. Accordingly, for the reasons set forth above with respect to claims 30, 37, 72, 79, 93, 99, 111, and 119, applicants respectfully submit that claims 135-154 should be allowable.

Serial No.: 10/785,584

CONCLUSION

In light of the above Amendments and Remarks, it is respectfully submitted that the present application is now in proper condition for allowance, and an early notice to such effect is earnestly solicited.

If any small matter should remain outstanding after the Patent Examiner has had an opportunity to review the above Remarks, the Patent Examiner is respectfully requested to telephone the undersigned patent attorney in order to resolve these matters and avoid the issuance of another Official Action.
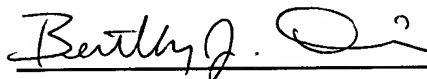
FEE DUE

A check in the amount of $1,050.00 is enclosed for the fee due. The Commissioner is authorized to charge any deficiencies of payment associated with the filing of this correspondence to Deposit Account No. **50-0426** to avoid the unintentional abandonment of the instant application.

Respectfully submitted,

JENKINS, WILSON, TAYLOR & HUNT, P.A.

Date: December 13, 2007   By: _Bentley J. Olive_

Bentley J. Olive
Registration No. 44,985
Customer No: 25297

919-493-8000

1503/7

- 44 -